# DID THE FBI HAVE A CHANCE TO FIX THEIR LIES ABOUT ENCRYPTION IN 2016?

The WaPo reports that the FBI has been presenting grossly inflated numbers describing how many devices it can't open because of encryption. The error stems, the FBI claims, to a "programming" error that actually sounds like an analytical error: the double or triple counting of the same encrypted phones.

> Over a period of seven months, FBI Director Christopher A. Wray cited the inflated figure as the most compelling evidence for the need to address what the FBI calls "Going Dark" — the spread of encrypted software that can block investigators' access to digital data even with a court order.
>
> The FBI first became aware of the miscount about a month ago and still does not have an accurate count of how many encrypted phones they received as part of criminal investigationslast year, officials said. Last week, one internal estimate put the correct number of locked phones at 1,200, though officials expect that number to change as they launch a new audit, which could take weeks to complete, according to people familiar with the work.
>
> "The FBI's initial assessment is that programming errors resulted in significant over-counting of mobile devices reported,'' the FBI said in a statement Tuesday. The bureau said the problem stemmed from the use of three distinct databases that led to repeated counting of phones. Tests of the methodology conducted in April 2016

> failed to detect the flaw, according to people familiar with the work.

I find the April 2016 failed test suspicious.

To know why, consider this bit of history. Back in 2015, in the wake of Apple making encryption standard, Jim Comey and Sally Yates made a big pitch for back doors. But when Al Franken asked them, they admitted the FBI didn't actually know how big the problem is.

> Over an hour and a quarter into the SJC hearing, Al Franken asked for actual data demonstrating how big of a problem encryption really is. Yates replied that the government doesn't track this data because once an agency discovers they're targeting a device with unbreakable encryption, they use other means of targeting. (Which seems to suggest the agencies *have* other means to pursue the targets, but Yates didn't acknowledge that.) So the agencies simply don't count how many times they run into encryption problems. "I don't have good enough numbers yet," Comey admitted when asked again at the later hearing about why FBI can't demonstrate this need with real data.

Nevertheless, in spite of Congress' request for real numbers in July 2015, in January 2016 — just as some at FBI were trying to create an excuse to force Apple to open Syen Rizwan Farook's phone — Comey and Yates admitted they still hadn't started tracking numbers.

> Around January 26, 2016 (that's the date shown for document creation in the PDF) — significantly, right as FBI was prepping to go after Syed Rizwan Farook's phone, but before it had done so — Comey and Yates finally answered the Questions for the Record submitted after the hearing. After claiming, in a

> response to a Grassley question on smart phones, “the data on the majority of the devices seized in the United States may no longer be accessible to law enforcement even with a court order or search warrant,” Comey then explained that they do not have the kind of statistical information Cy Vance claims to keep on phones they can’t access, explaining (over five months after promising to track such things),
>
> > As with the “data-in-motion” problem, the FBI is working on improving enterprise-wide quantitative data collection to better explain the “data-at-rest” problem.”
> >
> > [snip]
> >
> > As noted above, the FBI is currently working on improving enterprise-wide quantitative data collection to better understand and explain the “data at rest” problem. This process includes adopting new business processes to help track when devices are encountered that cannot be decrypted, and when we believe leads have been lost or investigations impeded because of our inability to obtain data.
> >
> > [snip]
> >
> > We agree that the FBI must institute better methods to measure these challenges when they occur.
> >
> > [snip]
> >
> > The FBI is working to identify new mechanisms to better capture and convey the challenges encountered with lawful access to both data-in-motion and data-

> at =-rest.

Grassley specifically asked Yates about the Wiretap report. She admitted that DOJ was still not collecting the information it promised to back in July.

> The Wiretap Report only reflects the number of criminal applications that are sought, and not the many instances in which an investigator is dissuaded from pursuing a court order by the knowledge that the information obtained will be encrypted and unreadable. That is, the Wiretap Report does not include statistics on cases in which the investigator does not pursue an interception order because the provider has asserted that an intercept solution does not exist. Obtaining a wiretap order in criminal investigations is extremely resource-intensive as it requires a huge investment in agent and attorney time, and the review process is extensive. It is not prudent for agents and prosecutors to devote resources to this task if they know in advance the targeted communications cannot be intercepted. The Wiretap Report, which applies solely to approved wiretaps, records only those extremely rare instances where agents and prosecutors obtain a wiretap order and are surprised when encryption prevents the court-ordered interception. It is also important to note that the Wiretap Report does not include data for wiretaps authorized as part of national

> security investigations.
>
> These two answers lay out why the numbers in the Wiretap Report are of limited value in assessing how big a problem encryption is.

Significantly, Comey and Yates offered these answers in response to a Chuck Grassley question about whether they believed, as the corrupt Cy Vance had claimed in Senate testimony, that "71% of all mobile devices examined…may be outside the reach of a warrant."

The number FBI is now trying to correct was "more than half," inching right up towards that 71% Vance floated years ago. In other words, this faulty methodology got them to where they needed to go.

I find that all the more suspicious given something that happened later in 2016. As soon as Jim Comey started providing numbers in August 2016, back when they showed 13% of phones could not be accessed, I asked how FBI came up with the number. At the time, a spox admitted that the number included more than encrypted phones — it also included deleted or destroyed phones.

> It is a reflection of data on the number of times over the course of each quarter this year that the FBI or one of our law enforcement partners (federal, state, local, or tribal) has sought assistance from FBI digital forensic examiners with respect to accessing data on various mobile devices where the device is locked, data was deleted or encrypted, the hardware was damaged, or there were other challenges with accessing the data. I am not able to break that down by crime type.

That is, in September 2016, five months after FBI failed to find their flawed methodology, an FBI spox told me the number used was not an

accurate count of how many phones couldn't be accessed because of encryption.

When then FBI General Counsel James Baker used the same 13% a few months later, claiming all were encrypted, I checked back. The same spox said the number at that point was *just* encrypted phones.

> It is true that damaged devices are provided to CART and RCFL for FBI assistance, but the 886 devices in FY16 that the FBI was not able to access (which is the number that GC Baker provided last week), does not include those damaged devices. It includes only those devices for which we encountered a password we were not able to bypass.

Now, it's possible that the methodological problem I identified in 2016 — that their "Going Dark" number actually included phones they couldn't access for entirely different reasons — was a different problem than the one just identified a month ago (just before Baker retired). Certainly, it doesn't sound like the same problem (though as I reminded someone from DOJ's IG some time ago, the forensics labs sending in these numbers have a history of unreliable numbers). That said, given the proliferation of chat apps with disappearing messages that amount to "destroyed" evidence — which under the flawed methodology used in 2016 would be counted as an encryption problem — it could be.

Still, what I identified in September 2016 *was* a methodological problem. It should have triggered a closer look at the time.

Instead, the FBI has been lying about how bad the Going Dark problem is for another year and a half.